AMENDMENTS TO THE CLAIMS

The Listing of Claims will replace all prior versions and listings of claims in the present patent application:

Listing of Claims

1. (Original) A method for secure wireless communication using spread spectrum principles, comprising:

generating at least one pseudorandom number (PN) sequence;
encrypting the PN sequence to render an encrypted PN sequence; and
using the encrypted PN sequence to spread a communication signal.

2. (Original) The method of Claim 1, wherein the communication signal is received from a data modulation component including a Walsh modulator.

3. (Original) The method of Claim 1, wherein the PN sequence is encrypted by combining the PN sequence with at least one encryption sequence.

4. (Original) The method of Claim 1, wherein one or more PN sequences are encrypted by combining the PN sequences with at least one encryption sequence.

5. (Original) The method of Claim 3, wherein the encryption sequence is generated by a DES or triple-DES encryption.

6. (Original) The method of Claim 5, wherein the DES or triple-DES encryption receives input including at least one multi-bit key and at least one time varying input.

7. (Original) The method of Claim 6, wherein the key is periodically refreshed.

8. (Original) A wireless communication system, comprising:

PAGE 3/11 * RCVD AT 3/24/2006 5:38:27 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/10 * DNIS:2738300 * CSID:858 845 2550 * DURATION (mm-ss):03-08

at least one data modulation component coding a communication signal for error correction to produce a coded signal, interleaving bits in the coded signal to produce an interleaved coded signal to reduce the effect of error bursts, and modulating the interleaved coded signal using a Walsh function to produce a Walsh-modulated interleaved coded signal; and

at least one carrier modulator for spreading the Walsh-modulated interleaved coded signal with a pseudorandom number (PN) sequence encrypted with at least one encryption sequence.

9. (Original) The system of Claim 8, comprising a PN generator generating the PN sequence and receiving the encryption sequence.

10. (Original) The system of Claim 8, comprising using two encryption sequences.

11. (Original) The system of Claim 8, comprising an encryption sequence generator generating the encryption sequence.

12. (Original) The system of Claim 11, wherein the encryption sequence generator includes a DES or triple-DES encryption.

13. (Original) The system of Claim 11, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.

14. (Original) A computer program product, comprising:

means for encrypting a PN sequence; and

means for providing the PN sequence to a spread spectrum communication device for use thereof in spreading or despreading a communication signal.

PAGE 4/11 * RCVD AT 3/24/2006 5:38:27 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/10 * DNIS:2738300 * CSID:858 845 2550 * DURATION (mm-ss):03-08

15. (Original) The product of Claim 14, wherein the communication device uses CDMA principles.

16. (Original) A chip for use in a communication device, comprising:

at least one data modulation component including:

at least one channel coder receiving a signal for communication, the channel coder coding the signal for error correction to produce a coded signal;

at least one bit interleaver coupled to the channel coder for interleaving bits in the coded signal to produce an interleaved coded signal to reduce the effect of error bursts;

at least one Walsh modulator coupled to the bit interleaver and modulating the interleaved coded signal using a Walsh function to produce a Walsh-modulated interleaved coded signal; and

at least one carrier modulator for spreading the Walsh-modulated interleaved coded signal with a pseudorandom number (PN) sequence encrypted with at least one encryption sequence.

17. (Original) The chip of Claim 16, comprising a PN generator generating the PN sequence and receiving the encryption sequence.

18. (Original) The chip of Claim 17, wherein the encryption sequence is a first sequence and the PN generator receives the first sequence and a second encryption sequence, the PN sequence being encrypted with both encryption sequences.

19. (Original) The chip of Claim 16, comprising an encryption sequence generator generating the encryption sequence.

20. (Original) The chip of Claim 19, wherein the encryption sequence generator includes a DES or triple-DES encryption.

PAGE 5/11 * RCVD AT 3/24/2006 5:38:27 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/10 * DNIS:2738300 * CSID:858 845 2550 * DURATION (mm-ss):03-08

21. (Original) The chip of Claim 19, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.

22. (Original) A chip for use in a communication device, comprising:

at least one PN sequence generator receiving at least one encryption sequence and combining the encryption sequence with a PN sequence to establish a combined sequence;

at least one carrier demodulator despreading a received spread spectrum communication signal using the combined sequence to render a despread signal; and

at least one data demodulation component coupled to the carrier demodulator to Walsh-process the despread signal, the demodulation component also deinterleaving the signal to render a deinterleaved signal and channel-demodulating the deinterleaved signal.

23. (Original) The chip of Claim 22, wherein the encryption sequence is a first sequence and the PN sequence generator receives the first sequence and a second encryption sequence.

24. (Original) The chip of Claim 23, comprising an encryption sequence generator generating the encryption sequence.

25. (Original) The chip of Claim 24, wherein the encryption sequence generator includes a DES or triple-DES encryption.

26. (Original) The chip of Claim 24, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.

27. (Original) A method for secure wireless communication using spread spectrum principles, comprising:

receiving at least one encryption sequence;

using the encryption sequence to render an encrypted PN sequence; and

PAGE 6/11 * RCVD AT 3/24/2006 5:38:27 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/10 * DNIS:2738300 * CSID:858 845 2550 * DURATION (mm-ss):03-08

using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

28. (Original) The method of Claim 27, wherein the despread signal is sent to a Walsh modulator.

29. (Original) The method of Claim 27, wherein the PN sequence is encrypted by combining the PN sequence with at least one encryption sequence.

30. (Original) The method of Claim 27, wherein one or more PN sequences are encrypted by combining the PN sequences with at least two encryption sequences.

31. (Original) The method of Claim 29, wherein the encryption sequence is generated by a DES or triple-DES encryption.

32. (Original) The method of Claim 31, wherein the DES or triple-DES encryption receives input including at least one multi-bit key and at least one varying input.

33. (Original) The method of Claim 32, wherein the key is periodically refreshed.

34. (Original) The method of Claim 32, wherein the varying input is at least one long code state.

PAGE 7/11 * RCVD AT 3/24/2006 5:38:27 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/10 * DNIS:2738300 * CSID:858 845 2550 * DURATION (mm-ss):03-08